Reliability Engineering and System Safety 210 (2021) 107545

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Safety systems for the oil and gas industrial facilities: Design, maintenance policy choice, and crew scheduling

Yury Redutskiy [a,*], Cecilie M. Camitz-Leidland [a], Anastasiia Vysochyna [a], Kristanna T. Anderson [a], Marina Balycheva [b]

[a] Molde University College – Specialized University in Logistics, P.O. Box 2110, NO-6402, Molde, Norway
[b] National University of Oil and Gas «Gubkin University», 65 Leninsky Prospekt, Moscow, 119991, Russia

ARTICLE INFO

Keywords:
Diverse redundancy
Engineering design
Maintenance planning
Markov analysis
Multi-objective optimization
Oil and gas industry
Remote and Arctic location
Requirements specification
Reliability engineering
Risk management
Safety instrumented system

ABSTRACT

The technology of oil and gas production is associated with significant hazards. Safety Instrumented Systems (SIS) are designed to ensure proper and safe operations in this sector. This research presents a framework that produces reasonable recommendations (requirements specification) for the SIS design and maintenance with consideration of the three key perspectives relevant to any petroleum engineering project, namely those of facility operators, engineering contractors, and the authorities. The contribution of this research to the area of engineering design is simultaneously addressing the decisions on the SIS design, organization of its maintenance, and employee scheduling for the remotely-located hazardous industrial facilities. These decisions are made based on the choice of maintenance policies incorporated into a Markov model of the system functioning. Another contribution of this research to the reliability modeling area is incorporating diverse redundancy into the modeling and decision-making framework. Thus, this research explores a trade-off between the capital investments into the SIS's design complexity and the operational expenditures associated with system maintenance and expected losses due to potential hazards. The developed multi-objective decision-making framework requires a black-box optimization approach to produce results. This research is relevant to engineering departments and contractors specializing in designing technological solutions for the petroleum sector.

1. Introduction

The demand for hydrocarbon energy worldwide has been increasing over the past few decades. At the same time, the oil and gas industry is facing a shift towards conducting operations in non-conventional locations. Examples of such production environments are remote, poorly accessible, offshore/deepwater, and Arctic locations. In recent decades, the petroleum reserves in the Arctic have become more accessible due to the ice melting, which resulted in increased international attention to this region [1]. Establishing facilities in these new environments and unpopulated areas is seen as beneficial for both businesses and societal welfare. On the other hand, these environments present considerable challenges to the oil and gas sector where operations are by default associated with potential hazards since they deal with flammable, toxic, and explosive substances, and therefore, pose risks to people, technological assets, environment, and companies' reputations.

Complex process automation and IT systems are deployed to ensure the proper course of hazardous industrial facilities' operations. A part of this IT solution is referred to as Safety Instrumented Systems (SIS). These systems act as protective barriers aiming either to prevent the occurrence of unwanted events or to mitigate the hazardous consequences. Among these systems, there are *process shutdown* systems which may isolate parts of the technology in semi-critical situations, *emergency shutdown* (ESD) systems which shut down the entire process in case an emergency condition which can quickly escalate to a critical situation, is identified, *fire and gas* systems which detect fire and high concentrations of hydrocarbon gases and notifies the personnel about it, *pressure protection* systems for pipelines, and potentially others [2]. Among these barriers, ESD systems are considered to be especially important as they provide the most substantial risk reduction among the preventive safety barriers [3].

The typical form of implementing a technological solution in the oil and gas industry is as an engineering project. Any project consists of several key phases, as described in [4–6]. A project is initiated by oil and gas exploration and production (E&P) operator company, and it starts with a *conceptual design* phase when some general information about the technology is gathered, hazard and risks are analyzed, and

* Corresponding author.
E-mail address: Yury.Redutskiy@HiMolde.no (Y. Redutskiy).

https://doi.org/10.1016/j.ress.2021.107545
Received 29 July 2020; Received in revised form 20 December 2020; Accepted 6 February 2021
Available online 12 February 2021

some insight is gained into the required safety barriers. The next stage is the development of safety requirements specification (SRS), which is a specialized document that has to be prepared for any kind of process automation and IT solution stating general requirements for different parts of the systems and their and functions. In the case of SRS, the requirements are determined for safety-related systems. These requirements are further followed when the *detailed engineering design* is performed. The development of the technical and technological solution is delegated to an engineering contractor company. After the solution has been developed, its *installation, commissioning and validation* are conducted to verify the proper performance of all the instrumentation and software. The longest-running phase of the solution's lifecycle may be referred to as *operations and maintenance* when the industrial facilities run their processes and produce revenues for the E&P companies. Maintaining technological equipment is a vital issue that ensures the safe and appropriate course for the activities, especially for hazardous technologies. The final phase in the system's lifecycle is the proper facility *decommissioning*.

Incidents happen quite often in the oil and gas industry. A detailed analysis of a sample of incidents [7] traced their primary cause back to the inadequacies during the *requirement specification* phase of the engineering project in almost half of the studied cases. The study concludes that the lack of clear, sufficient, and comprehensive requirements led to the inadequate safety level that the designed automated system could provide for the processes.

To provide comprehensive requirements to SISs, safety measures inherent in them have to be analyzed. The specifics of the SISs are determined by two international standards: IEC 61508 and IEC 61511. These standards focus on how the necessary level of safety may be achieved by making decisions regarding certain SIS features. Designing an SIS implies choosing certain instrumentation, determining architectural specifics, and planning the system's maintenance. Based on the mentioned standards, national regulations in every country impose general requirements to the safety level on various hazardous technologies. The examples of these regulations [8,9] show that the suggested requirements are somewhat broad. To define clear and comprehensive requirements for the safety of industrial facilities, the recommendations should be provided to specific aspects of the SIS given the nature of the measures it comprises. It would provide a reasonably good foundation for the detailed engineering design of the solution.

The issue of maintenance should be paid especially close attention given the modern-day oil and gas industry's challenges, now that the operations are shifting to remote and poorly accessible locations [10]. To provide service for such facilities, the maintenance personnel works in shifts: crews of engineers are transported to the remotely-located facilities to conduct the testing. In this context, the transportation costs are expected to play a considerable role in the decision-making concerning the specifics of the designed SIS [11].

This research aims to address the issue of choosing the appropriate set of safety measures inherent in SIS to facilitate the *requirements specification* development by formulating a clear and comprehensive approach to SIS design and maintenance. To fulfill this purpose, first, a brief review of safety and reliability issues in the oil and gas industry is conducted, as well as the review of employee scheduling issues that are relevant to the modern-day industrial solutions in remote locations. And second, a decision-making framework is developed to address the design with its technical challenges and specifics together with maintenance planning and its organization by means of employee scheduling.

2. Overview of the research area

A considerable body of research in the area of SIS design has been accumulated over the past three decades. The research in this area is primarily based on methods of reliability quantification. The international standards [12] and [13] gather fundamental ideas and methodological approaches to safety modeling. The standards refer to such methods as *reliability block diagrams* (RBD) and *fault tree analysis* (FTA) as straightforward and visual modeling tools. However, due to the simplicity of these approaches, they have certain limitations. That is why some researchers use *Markov analysis* as it is a flexible approach allowing to cover various intricacies of the SIS performance [5,6,14–17]. An interested reader may refer to Kuo and Zuo [18] for an extensive overview and a comparison of approaches to modeling and design of industrial safety systems. The reader may also refer to Gabriel et al. [19] for an overview of the state-of-the-art research and the trends in the area of SIS modeling and design.

One of the key concepts in the SIS design is redundancy. It implies using more than one device to perform the same function aiming to improve the system availability. Research [20] and recent papers [21,22] point out that the overwhelming majority of available papers focus exclusively on redundancies with identical components. From the viewpoint of engineering practice, using only identical devices is not a widely accepted approach. Few researchers, namely [20–25], have attempted to incorporate diverse components into the redundancy architectures. They show that instrumentation diversity improves the overall system's reliability. However, the mentioned research on diverse redundancy or component mixing focuses exclusively on the system design, thereby deflecting from considering the issues of maintenance during the course of operations. In the mentioned research, heterogeneous redundancy architectures are studied with the help of the RBD and FTA methods, which are not tailored for repairable systems. Very few papers [25–27] attempt to incorporate device repairs in their models. Notably, Khatab et al. [25] apply Markov analysis, a technique suitable for addressing repairable systems. The authors develop a specialized model capable of recognizing the failed components and prioritizing the repairs. The research presented further in this paper also utilizes Markov analysis due to the strong focus on maintenance details. However, there will be no need for repair priorities as the corrective maintenance is normally organized following the first-in-first-out principle.

Besides addressing an industrial safety system from the reliability viewpoint, this paper covers the issue of maintenance and, specifically, the aspect of employee scheduling, which is relevant to remotely-located industrial facilities. The area of employee scheduling has been widely developed since the middle of the 20th century when a set-covering employee scheduling model was proposed by Dantzig [28]. An interested reader may refer to the papers [29,30] as extensive overviews of the various workforce organization and scheduling issues, applications, models, and solution approaches. Among the various contexts, a class of problems called *workforce scheduling and routing* is identified. This class addresses the requirement for personnel to perform a given service at a given location. An important feature of this problem category is that the demand has to be satisfied precisely, unlike in many other real-life settings. An interested reader is also encouraged to refer to research [31] for a good review of the issues relevant to such problem contexts.

When a safety system design is addressed, a certain level of operational details (such as planning repairs) is taken into account. When a new industrial engineering project is initiated, it is essential to address the workforce-related decisions with respect to the engineering design, which influences the personnel requirements as well as scheduling the shift work. Authors Helber and Henken [32] emphasize that such joint decision-making helps explore trade-offs between the process performance and the workforce-related costs. Finding this trade-off would be impossible, if the focus is placed solely on the aspects of crew scheduling and routing as it is done in the research mentioned in the previous paragraph. Therefore, further the workforce planning issues are addressed together with the engineering design aspects.

This research takes into account designing an SIS with heterogeneous redundancy architectures, planning the system's maintenance,

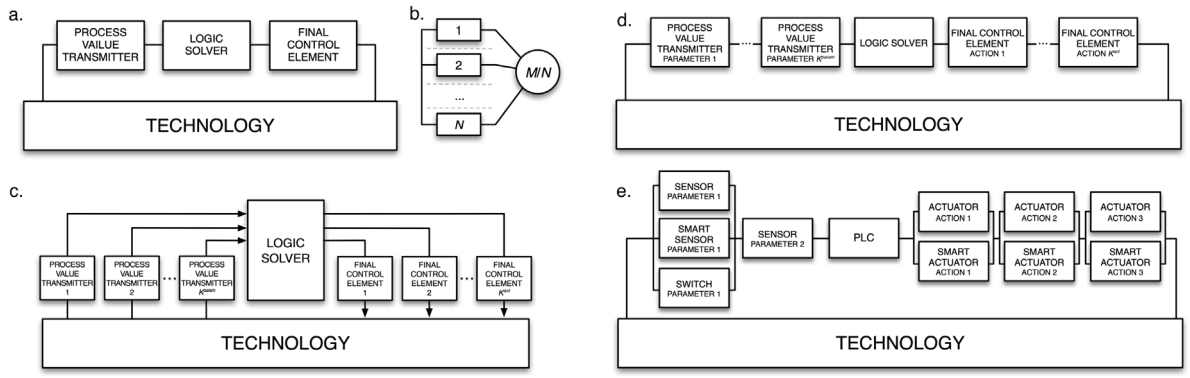

Fig. 1. SIS structure. Based on IEC 61508 and 61511. a. Control loop. b. MooN architecture. c. Real-life SIS physical structure. d. Real-life SIS structure (RBD). e. SIS with diverse redundancy (RBD).

and organizing the workforce — all within one decision-making framework. It allows balancing the investments into the system's complexity, the achieved level of safety, and the workforce-related costs. Markov analysis is employed to model various aspects of the emergency shutdown system functioning with a particular hazardous technology. Further, the personnel requirements and the solution's lifecycle cost are evaluated. Continuing research [5,6,11], multi-objective decision-making is applied to produce results and reveal tendencies and features of the best solutions, which may facilitate developing clear and comprehensive requirements to the SIS design, maintenance, and workforce planning.

3. Modeling and decision-making framework for SIS design and maintenance organization

3.1. Problem setting

Safety instrumented system design

According to the international standards [12] and [13], any safety instrumented system by definition consists of three types of subsystems performing the following functions (see Fig. 1a): (a) *process value transmitters*, or, simply put, *sensors* measuring technological parameters and delivering their values to the next subsystem: (b) *logic solvers*, or in other words, *programmable logic controllers* (PLC) which implement a certain control algorithm, given the values of the process parameters. The output signals generated by the PLCs get delivered to the next subsystem: (c) *final control elements*, or simply put, *actuators*. These devices are vales, drives, switches, etc., which assign certain operating modes to the actual technological facilities and units.

The loop in Fig. 1a shows only one subsystem of each described type. For real-life technological solutions, a safety system is likely to keep track of several process values simultaneously. It means that there should be several sensor subsystems for different parameters put in place. Also, when critical situations occur, it is common that multiple actions are taken, and therefore, several actuator subsystems have to be included in the SIS. The signals from all the sensors are delivered to the controller subsystem, which, in turn, is responsible for operating multiple actuators. It is reflected in Fig. 1c.

From the reliability block-diagram (RBD) perspective, the structure reflected in Fig. 1c should be presented as a sequential connection of all the subsystems, as demonstrated in Fig. 1d. It implies that the SIS may only perform its function fully when all of its subsystems are properly operating.

The design of a particular automated safety system implies making choices regarding the specifics of the SIS's subsystems. These choices include:

- *Device models* for sensor, controller, and actuator subsystems. For any kind of device, several analogous options manufactured by different vendors (brands like Emerson, Honeywell, Siemens, Yokogawa, ABB, etc.) are available on the market. Although these functionally analogous devices perform the same task, the reliability characteristics and costs of the devices produced by different manufacturers often vary considerably.
- *Redundancy architectures*: each SIS's subsystem depicted as blocks in Fig. 1a,c,d may consist of one or more identical devices. Using more than one device in a particular subsystem allows the subsystem to stay operational when some devices fail, while others keep performing. The redundancy description is most often done through M-out-of-N (MooN) architectures (Fig. 1b), where N stands for the total number of components, and M stands for the number of devices required to function properly so that the entire subsystem would be considered functional.
- *Additional device separation* (electrical, physical, or both) within a redundancy architecture is often introduced to reduce the effect of the common-cause failures (CCF) when all the components in the architecture fail simultaneously. In Fig. 1b, the additional separation is represented by the dashed lines between the devices.

Designing an automated safety system based on the measures described so far results in the SIS's subsystems being blocks of identical devices. In engineering practice, this is rarely the case, especially when it concerns field devices, i.e., sensors and actuators. When more than one component has to be employed to perform a particular function, the devices of different nature are often used. For example, to signal a critically high liquid level in a tank or a processing unit, a continuous-value level sensor may be used as well as a level switch set up to the required critical level mark. In addition, among many continuous-value transmitters, ordinary sensors and smart sensors may be distinguished. The latter are more expensive, but at the same time, they exhibit better reliability performance.

A simple approach to including the possibility of using different-nature devices into the SIS decision-making context, several MooN architectures, each standing for its own device type, may be used in parallel as demonstrated in Fig. 1e. The blocks of diverse devices performing the same function should be connected in parallel from the RBD viewpoint.

The example in Fig. 1e shows two sensor subsystems. For the first subsystem, diverse redundancy is utilized: ordinary, smart sensors, and switches are selected. For the second sensor subsystem, the diverse redundancy is not used. For the three actuator subsystems, diverse redundancy with two different kinds of actuators – standard and smart – are chosen.

Planning SIS maintenance and facility overhauls

Planning the maintenance of the SIS is another vital aspect of the technological solution's performance. Safety system maintenance is done:

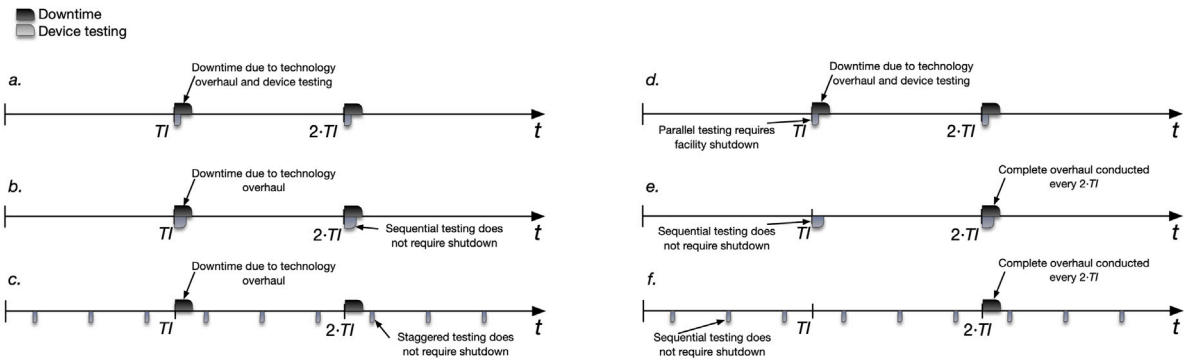

Fig. 2. a, d: parallel testing; b, e: sequential testing; b, f: staggered testing with the uniformly distributed tests. a, b, c: technology overhaul period equals TI; d, e, f: technology overhaul period equals 2·TI. Based on Torres-Echeverria et al. [20].

- *continuously* to resolve the failures that are revealed while the technology runs, e.g., by self-diagnostic function, or from the situations which lead to the safety system's tripping.
- *periodically* to resolve all the problems that are unrevealed during the normal course of operations. The period of conducting these proof tests is called the *test interval* (TI).

It is beneficial to perform planning the design of an SIS together with its maintenance. These aspects are both associated with considerable expenditures, and therefore, it may prove useful to explore the trade-off between them. Highly reliable equipment or complex redundancy architectures are often quite expensive, however, they will most likely not require frequent maintenance. Cheaper SIS instrumentation and simpler redundancies are likely to require frequent proof tests. The former brings about large capital expenses. The latter leads to considerable operational costs associated with labor (especially for remotely-located facilities), spare parts, and necessary maintenance tools together with potential losses due to the facility downtime for the duration of the maintenance. While performing long-term planning, both SIS design, maintenance planning, and labor organization aspects should be considered within one decision-making framework.

In addition to choosing maintenance frequency (or its inverse – test interval), a decision on the approach to proof testing, called *maintenance policy*, should also be considered. Fig. 2 demonstrates three proof testing policies: parallel testing, sequential testing, and staggered testing with the tests uniformly distributed within the test interval. The parallel testing policy implies that testing of all the devices in the SIS is started simultaneously. The sequential testing policy implies that testing the devices within each subsystem is done one by one by the same maintenance engineer. It is, therefore, obvious that sequential proof testing requires fewer workers to be present at the facility for the testing period, however, the testing itself should take a longer time, which extends the technology downtime. Another approach to testing is the staggered policy when the devices in each subsystem are tested at separate points in time within the test interval. There may be other testing policies (such as partial testing) as well as many different approaches to staggered testing. In this research, decision-making is limited to the instrumentation testing approaches presented in Fig. 2.

One may observe from Fig. 2 that in addition to maintaining the SIS instrumentation, the technological units should also be maintained at certain points. The model presented further considers the period between two consecutive technological overhauls – the *overhaul period* (OP) – to be equal to the value of TI or a multiple of TI.

This research utilizes Markov modeling to quantify the safety system's performance in terms of reliability modeling. An assumption crucial for Markov analysis is the exponential distribution of the stochastically occurring events, which are device failures and repairs, as well as technological incidents and restorations. This assumption may be represented with Eqs. (1). The exponential distribution of the failures and incidents is assumed valid for complex systems, especially those involving electric and electronic devices [33]. Researcher [14] states that the exponential distribution of repairs and restorations is a slightly optimistic assumption for real-life cases. In this research, a pessimistic assumption is made regarding the repair rates and the average repair times based on the suggestion proposed in [5].

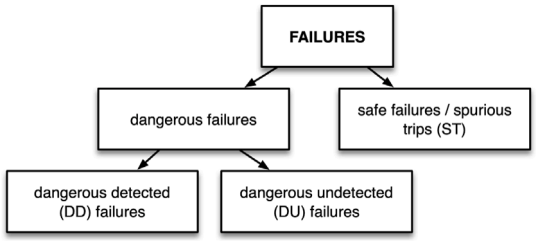

Fig. 3. Classification of the failure modes assumed for this research. *Source:* Adopted from [5,6].

$$P^{event}(t) = 1 - e^{-\lambda \cdot t}, \quad t \geq 0 \tag{1}$$

Fig. 3 demonstrates the classification of failures assumed for this research. The important aspect of this particular classification is that all the safe failures are considered to be detected failures. This assumption is quite reasonable for an SIS, such as an emergency shutdown system. In case of a safe failure, the ESD system shuts down the technology, which cannot go undetected.

Workforce organization

As mentioned earlier, decisions regarding the maintenance of the SIS solutions are crucial to their performance. Since the maintenance is performed by the engineers who specialize in working with the automated systems, organizing the workforce to implement the necessary maintenance becomes vital for the modern-day facilities and production sites located quite far from cities and large industrial centers. To address this problem, in many cases, a subsidiary of an operating company is established somewhat close to the production site or the remote facility location, and the local engineers get trained to perform the SIS and facility maintenance. Nevertheless, it often takes several transportation modes and legs and to deliver the personnel to the facilities and back. To address planning the workforce to run the required maintenance, this research utilizes the set-covering formulation of the employee scheduling model proposed by Dantzig [28]. This model implies defining a set of shifts, or in our case, trip durations to the remote location, and it determines how many crews should take a trip of a particular duration starting at a particular point in time. This type of employee scheduling model utilizes the approach of "hard demand constraints" when the demand for the number of employees required to be present at the facility at a certain point in the planning horizon has to be satisfied exactly. This approach is suitable for oil and

Table 1
SIL requirements suggested by IEC [12] and IEC [13].

SIL	Risk reduction requirement		Fault tolerance requirement[a] for logic solvers			Fault tolerance requirement[a]
	PFD_{avg}	RRF[b]	With $SFF < 60\%$	With $60\% \leqslant SFF < 90\%$	With $SFF \geqslant 90\%$	for sensors and actuators
1	$[10^{-2},\ 10^{-1})$	$(10,\ 10^{2}]$	1	0	0	0
2	$[10^{-3},\ 10^{-2})$	$(10^{2},\ 10^{3}]$	2	1	0	1
3	$[10^{-4},\ 10^{-3})$	$(10^{3},\ 10^{4}]$	3	2	1	2
4	$[10^{-5},\ 10^{-4})$	$(10^{4},\ 10^{5}]$	Special requirements			Special requirements

[a]Refer to IEC [12] for explanation of fault tolerance requirement and safe failure fraction (SFF).
[b]Risk reduction factor.

gas industrial facilities since the maintenance requirements are usually stated quite strictly: a certain type of maintenance must be completed within the pre-defined timeframe. These timeframe requirements for testing and repairing, as well as the SIS design specifics, are used in the model to calculate the weekly demand for the number of employees required to be present at the facility during each week of the planning horizon.

The employee scheduling formulation proposed by Dantzig is modified in this research to accounts for certain specifics. The model proposed further accounts for compensation for longer shift durations for the employees since it has become a standard practice in the oil and gas companies to award employees who spend more time on trips with larger yearly or quarterly bonuses. Also, the model in this paper accounts for the decision of the daily schedule of work, which is related to the maintenance crew size. The choice is made between 8-hour working day during the trip to the remote location (in which case three workers are required to be in a maintenance crew to ensure the continuous 24-hour service), and 12-hour working day (in which case two workers are required to be in the crew). The model also accounts for establishing a workforce of a given size, providing the salaries and limiting the amount of time spent on trips to the remotely located facilities.

Multi-objective decision-making framework

To quantify the safety of a certain SIS solution, two reliability indicators are produced from the modeling framework presented further. One of these indicators is the *average probability of failure on demand* (PFD_{avg}) for which the requirements are set by the international standards in the form of the generalized safety integrity level (SIL), as well as national authorities' regulations for the hazardous industrial facilities. The requirements to SIL for the automated safety systems operating in so-called "low-demand mode" (when the frequency of incidents is no higher than once a year, according to IEC 61508) may be found in Table 1. The regulations imposed by national authorities, examples of which may be found in [8,9], for main processes within oil and gas production, processing, transportation, and refining technology, the required SIL is 3.

Another safety indicator considered in this research and produced by the Markov analysis is the expected facility *downtime* (DT). This indicator partly reflects the perspective of the company operating the oil and gas facility for whom the SIS is designed. The operator's goal is profit in the long run, making them strive for smooth operations of their technology.

Given the significant role of automated systems, especially the ESD system, which aims to prevent the technological incidents from occurring, many aspects are taken into consideration while the hazardous industrial facilities are planned for long-term operations. To consider the importance of these aspects (design complexity, maintenance strategy, and workforce organization), the economic perspective on the technical solution's lifecycle is suggested by the international standards. To address all the vital aspects of the long-term planning, the lifecycle cost of a safety instrumented system operating together with a particular hazardous technology should include the capital costs (or, in other words, procurement cost), the operational costs, as well as the risk costs. The latter cost category is specific to operations of the safety systems, and it describes the negative effects of the SIS and evaluates the expected losses in case a technological incident occurs.

The modeling and decision-making framework developed in this research consists of several blocks addressing various aspects of the long-term planning of an SIS. These blocks, as well as the decision variables and the objective functions for the optimization problem, are reflected in Fig. 4.

Decision variables:

- particular device models for each redundancy block of diverse-redundant structures for field device subsystems (transmitters and final control elements), as well as device model choice for the subsystem of logic solvers
- redundancy architecture (MooN) for each redundant block of each subsystem
- additional electric separation for each redundant block of each subsystem
- test interval (TI) for periodic proof testing and overhaul period (OP) as a multiple of TI
- proof testing policy (parallel, sequential, or staggered) for each redundancy block of each subsystem.

Given the stakeholders' viewpoints that need to be maintained for the real-life problem of designing and planning the maintenance for an SIS, the three following objective functions are used for the decision-making:

- minimizing the SIS's average probability of failure on demand
- minimizing the expected facility downtime
- minimizing the lifecycle cost of an SIS operating for a particular hazardous technology.

This paper continues the research [5,6,11]. Here, the lifecycle viewpoint suggested in the earlier research is still maintained for the strategic planning of the automated safety solutions employed for hazardous oil and gas industry technologies. This research, however, incorporates the possibility of diverse redundancy relevant to the field device subsystems (sensors and actuators). This paper also includes a more detailed view of the maintenance policies by incorporating the details of parallel, sequential, and staggered testing policies into the modeling framework.

3.2. Failures and repairs in an MooN architecture and a subsystem with diverse redundancy

A subsystem with only identical is represented as a single MooN architecture. A subsystem with diverse redundancy includes several MooN architectures. Therefore, modeling of the device failures and repairs begins with addressing one MooN architecture. Fig. 5a shows that the Markov model includes $(N - M + 2)$ states. State 1 stands for all N components operating properly. State 2 corresponds to one failure. Each further state represents one more device failure. The failure of the entire redundancy architecture is represented by the last absorbing state $(N - M + 2)$ corresponding to $(N - M + 1)$ failures. Independent failures are depicted by sequential left-to-right transitions on the graph, while common cause failures are depicted by the direct transition to the absorbing state. Device repairs are depicted by the backward transitions.

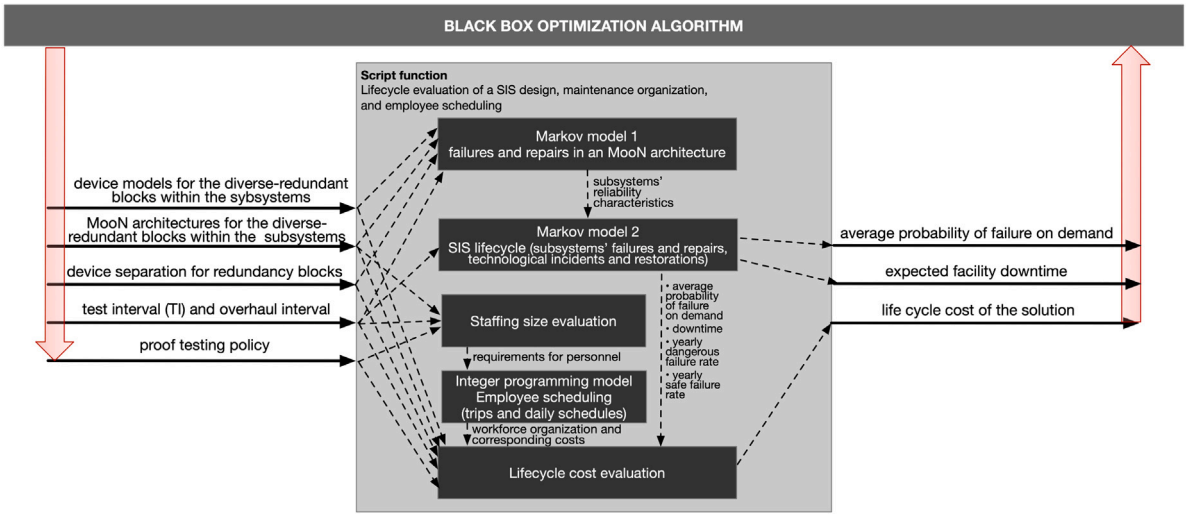

Fig. 4. Multi-objective decision-making framework. Based on Redutskiy [11].

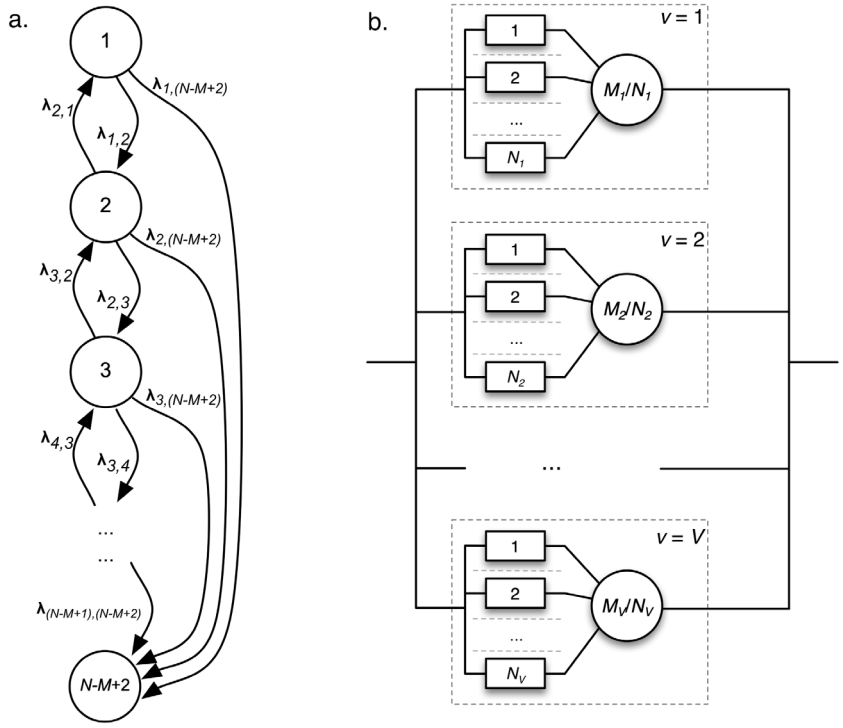

Fig. 5. Failures and repairs in a subsystem. a. Markov process of failures and repairs in an MooN architecture. b. A subsystem with diverse redundancy.

All the relevant notations for the modeling block presented in this section, are provided in Table 2. The time horizon for the model is equal to the duration of the test interval. Markov model equations are presented further separately for the three modeled failure modes: (2)–(6) for DU failures, (7)–(9) for DD failures, and (10)–(12) for ST in the MooN architecture.

For any failure mode, the probabilities of the redundancy architectures being in a particular state of the Markov model are described by a set of ordinary differential equations (ODE) shown in (2), (7) and (10), also known as Kolmogorov forward equations. The non-zero transition rates are also provided in (3), (8), and (11) for the three failure modes. The starting point of the stochastic process at $t = 0$ is State 1. The choice of the proof testing policy has an impact on how the Markov model is run for the case of the dangerous undetected failures, i.e., Eqs. (4)–(6). It is first and foremost due to the fact that the proof testing is conducted precisely to reveal the undetected failures. Also, when it comes to testing the devices, the models for the DD and ST failure modes are, in principle, also affected by testing the devices. However, the most important outcome of these Markov models is the value of the probability of the stochastic process being in the last (absorbing) state at the time $t = TI$, which ultimately reflects the reliability of the entire MooN architecture. Whatever policy is chosen for the proof testing, it does not affect these values. For the DU failure mode, the initial probabilities are defined in (4), (5), and (6) for the parallel, sequential, and staggered tests respectively. The models for the DD and ST failure modes do not require any modifications to estimate the architecture's respective reliability characteristics properly.

Having produced the values of probabilities of the stochastic process being in the state $(N - M + 2)$ for the DU, DD and ST failures, the corresponding failure rates are obtained in (13) given the assumption

of the failures' exponential distribution. In case a subsystem consists only of identical components, the values produced in expressions (13) are the output of this modeling block.

When considering diverse redundancy, the probabilities of the MooN architectures being in the absorbing state of the Markov model should be multiplied to account for several parallel MooN architectures failing simultaneously (Fig. 5b). Then, to account for diverse redundancy, expressions (13) should transform to (14).

Markov model for dangerous undetected failures in an MooN architecture:

$$\frac{dp_j^{DU}(t)}{dt} = \sum_{i=1}^{N-M+2} p_i^{DU}(t)\cdot\lambda_{i,j}^{DU}, \quad j\in\{1,\dots,(N-M+2)\} \tag{2}$$

$$\begin{aligned}
&\lambda_{i,i}^{DU} = -\lambda\cdot(1-\epsilon)\cdot[(N-i+1)\cdot(1-\beta)+\beta],\\
&\lambda_{i,i+1}^{DU} = \lambda\cdot(1-\epsilon)\cdot(N-i+1)\cdot(1-\beta),\\
&\lambda_{i,(N-M+2)}^{DU} = \lambda\cdot(1-\epsilon)\cdot\beta, \quad i\in\{1,\dots,(N-M+2)\}
\end{aligned} \tag{3}$$

$$p_1^{DU}(0)=1, \quad p_i^{DU}(0)=0; \quad i\in\{2,\dots,(N-M+2)\} \tag{4}$$

$$\begin{aligned}
&\pi_1^1=1, \quad \pi_i^1=0; \quad i\in\{2,\dots,(N-M+2)\}.\\
&\pi_1^k = p_1^{DU}\left((k-1)\cdot T^{TR}\right)+\tfrac{1}{N}\cdot p_2^{DU}\left((k-1)\cdot T^{TR}\right),\dots,\\
&\pi_{N-M+1}^k = p_{N-M+1}^{DU}\left((k-1)\cdot T^{TR}\right)+\tfrac{N-M+1}{N}\cdot p_{N-M+1}^{DU}\left((k-1)\cdot T^{TR}\right),\\
&\pi_{N-M+2}^k = 0; \quad k\in\{2,\dots,N\}.
\end{aligned} \tag{5}$$

$$\begin{aligned}
&\pi_1^1=1, \quad \pi_i^1=0; \quad i\in\{2,\dots,(N-M+2)\}.\\
&\pi_1^k = p_1^{DU}\left(\tfrac{(k-1)\cdot TI}{2\cdot N}\right)+\tfrac{1}{N}\cdot p_2^{DU}\left(\tfrac{(k-1)\cdot TI}{2\cdot N}\right),\dots,\\
&\pi_{N-M+1}^k = \tfrac{1}{N}\cdot p_{N-M+1}^{DU}\left(\tfrac{(k-1)\cdot TI}{2\cdot N}\right)+\tfrac{N-M+1}{N}\cdot p_{N-M+2}^{DU}\left(\tfrac{(k-1)\cdot TI}{2\cdot N}\right),\\
&\pi_{N-M+2}^k = 0; \quad k\in\{2,\dots,N\}.
\end{aligned} \tag{6}$$

Markov model for dangerous detected failures in an MooN architecture:

$$\frac{dp_j^{DD}(t)}{dt} = \sum_{i=1}^{N-M+2} p_i^{DD}(t)\cdot\lambda_{i,j}^{DD}, \quad j\in\{1,\dots,(N-M+2)\} \tag{7}$$

$$\begin{aligned}
&\lambda_{1,1}^{DD} = -\lambda\cdot\epsilon\cdot[N\cdot(1-\beta)+\beta], \quad \lambda_{1,2}^{DD} = \lambda\cdot\epsilon\cdot N\cdot(1-\beta),\\
&\lambda_{1,(N-M+2)}^{DD} = \lambda\cdot\epsilon\cdot\beta,\\
&\lambda_{i,i-1}^{DD} = (i-1)\cdot\mu, \quad \lambda_{i,i}^{DD} = -\lambda\cdot\epsilon\cdot[(N-i+1)\cdot(1-\beta)+\beta]-(i-1)\cdot\mu,\\
&\lambda_{i,i+1}^{DD} = \lambda\cdot\epsilon\cdot(N-i+1)\cdot(1-\beta), \quad \lambda_{i,(N-M+2)}^{DD} = \lambda\cdot\epsilon\cdot\beta,\\
&i\in\{2,\dots,(N-M+2)\}
\end{aligned} \tag{8}$$

$$p_1^{DD}(0)=1, \quad p_i^{DD}(0)=0; \quad i\in\{2,\dots,(N-M+2)\} \tag{9}$$

Markov model for spurious trips in an MooN architecture:

$$\frac{dp_j^{ST}(t)}{dt} = \sum_{i=1}^{N-M+2} p_i^{ST}(t)\cdot\lambda_{i,j}^{ST}, \quad j\in\{1,\dots,(N-M+2)\}. \tag{10}$$

$$\begin{aligned}
&\lambda_{1,1}^{ST} = -\lambda^S\cdot[N\cdot(1-\beta)+\beta], \quad \lambda_{1,2}^{ST} = \lambda^S\cdot N\cdot(1-\beta),\\
&\lambda_{1,(N-M+2)}^{ST} = \lambda^S\cdot\beta,\\
&\lambda_{i,i-1}^{ST} = (i-1)\cdot\mu, \quad \lambda_{i,i}^{ST} = -\lambda^S\cdot[(N-i+1)\cdot(1-\beta)+\beta]-(i-1)\cdot\mu,\\
&\lambda_{i,i+1}^{ST} = \lambda^S\cdot(N-i+1)\cdot(1-\beta), \quad \lambda_{i,(N-M+2)}^{ST} = \lambda^S\cdot\beta,\\
&i\in\{2,\dots,(N-M+2)\}
\end{aligned} \tag{11}$$

$$p_1^{ST}(0)=1, \quad p_i^{ST}(0)=0; \quad i\in\{2,\dots,(N-M+2)\} \tag{12}$$

Table 2
Notations used for the subsystem modeling.

Notations for failure modes	
DU	Dangerous undetected failures
DD	Dangerous detected failures
ST	Spurious trips/safe failures
Indices and parameters	
i, j	Indices for the Markov model states
k	Index for the devices and device maintenance time intervals for sequential and staggered testing policies, $k\in\{1..N\}$
υ	Index for the MooN architectures (with identical devices) within the subsystem with diverse redundancy, $\upsilon\in\{1..V\}$
N	Total number of components in MooN redundancy architecture
M	Necessary number of operating devices in MooN architecture
V	Total number of devices of various nature in the subsystem with diverse redundancy
TI	Test interval, h
T^{TR}	Time required for testing and repairing one component in the architecture, h
λ	Dangerous failure rate for one component, h^{-1}
λ^S	Spurious trip rate for one component, h^{-1}
μ	Repair rate, h^{-1}
ϵ	Diagnostic coverage, fraction
β	Common cause failure factor, fraction
$\lambda_{i,j}^{DU}$	Transition rates for the model of dangerous undetected failures, h^{-1}
$\lambda_{i,j}^{DD}$	Transition rates for the model of dangerous detected failures, h^{-1}
$\lambda_{i,j}^{ST}$	Transition rates for the model of spurious trips, h^{-1}
Variables	
t	Time, [h]
$p_j^{DU}(t)$	Probability of $(j-1)$ dangerous undetected failures
$p_j^{DD}(t)$	Probability of $(j-1)$ dangerous detected failures
$p_j^{ST}(t)$	Probability of $(j-1)$ spurious trips in a subsystem
$p_{\upsilon,j}^{DU}(t)$	Probability of $(j-1)$ dangerous undetected failures in the υth MooN architecture within the subsystem with diverse redundancy
$p_{\upsilon,j}^{DD}(t)$	Probability of $(j-1)$ dangerous detected failures in the υth MooN architecture within the subsystem with diverse redundancy
$p_{\upsilon,j}^{ST}(t)$	Probability of $(j-1)$ spurious trips in a subsystem in the υth MooN architecture within the subsystem with diverse redundancy
π_i^k	Initial probability of the Markov model's ith state after testing k devices (for sequential or staggered policy)
Outputs of the model	
λ^{DU}	Dangerous undetected failure rate for a subsystem, h^{-1}
λ^{DD}	Dangerous detected failure rate for a subsystem, h^{-1}
λ^{ST}	Spurious tripping rate for a subsystem, h^{-1}

Modeling output for an MooN architecture and for a subsystem with diverse redundancy:

$$\begin{aligned}
&\lambda^{DU} = -\frac{\log\left(1-p_{N-M+2}^{DU}(TI)\right)}{TI}, \quad \lambda^{DD} = -\frac{\log\left(1-p_{N-M+2}^{DD}(TI)\right)}{TI},\\
&\lambda^{ST} = -\frac{\log\left(1-p_{N-M+2}^{ST}(TI)\right)}{TI}
\end{aligned} \tag{13}$$

$$\begin{aligned}
&\lambda^{DU} = -\frac{\log\left(1-\prod_{\upsilon=1}^{V} p_{\upsilon,(N-M+2)}^{DU}(TI)\right)}{TI},\\
&\lambda^{DD} = -\frac{\log\left(1-\prod_{\upsilon=1}^{V} p_{\upsilon,(N-M+2)}^{DD}(TI)\right)}{TI},\\
&\lambda^{ST} = -\frac{\log\left(1-\prod_{\upsilon=1}^{V} p_{\upsilon,(N-M+2)}^{ST}(TI)\right)}{TI}
\end{aligned} \tag{14}$$

3.3. Lifecycle modeling from the safety perspective

Lifecycle model presented further is mostly adopted from [5,6].

From the modeling block described in the previous subsection, one may conclude that any subsystem of the SIS may either operate properly, or fail in a DU, DD, or ST way. At the same time, the technological facility may either be up and running, or shut down. The worst situation

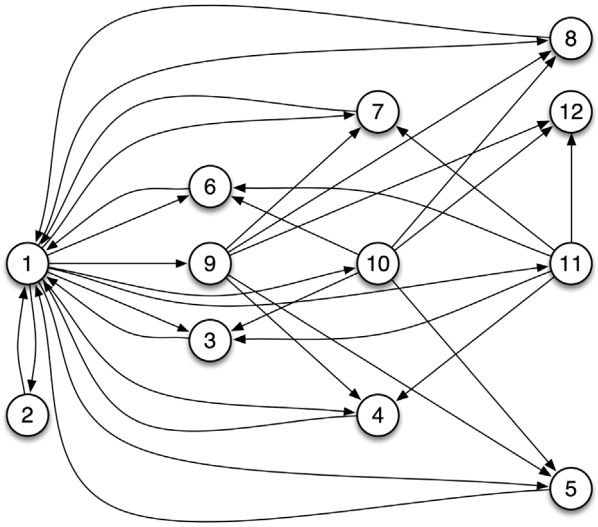

Fig. 6. Markov model of the lifecycle.
Source: Redutskiy [5,6]

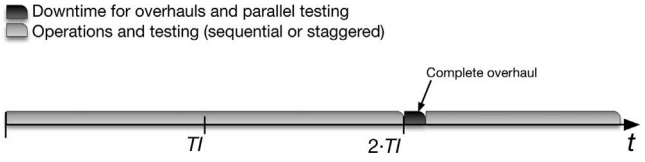

Fig. 7. Example of the time horizon for lifecycle modeling with overhaul period equal to $2 \cdot TI$.

is when a technological incident occurs, and the SIS does not perform the intended process shutdown due to one of the subsystems being in the DU failure state. Then, the operations at the facility proceed, which may lead to considerable hazardous consequences. This situation is called the failure-on-demand state of the process.

The details of all the states possible for the technology and the SIS are explained in Table 3 and all the transitions between the states of the stochastic process are depicted on the graph in Fig. 6. This description applies only to an SIS depicted in Fig. 1a, i.e., the one consisting of exactly three basic subsystems. The description of the stochastic process needs to be expanded for SISs like depicted in Fig. 1d,e. States 1 and 2 as well as the last absorbing state will always be present in the Markov model. The remaining states must account for the possibility of each subsystem's DU, DD, and ST failures. Therefore, the number of these remaining states will be dependent on the number of subsystems in the SIS. For the example with six subsystems in Fig. 1e, the Markov process will comprise 21 states.

Further, the mathematical model of the switching Markov process is presented for the basic configuration of the SIS (i.e., comprising three subsystems). The notations for this model are provided in Table 4.

The lifecycle of the technological solution is divided into K intervals (15) to account for periodic maintenance of the SIS and facility overhauls. The choice of the overhaul period (OP) is influenced by the chosen proof testing policy. If parallel testing policy is chosen for any subsystem, i.e., all the devices in the SIS are tested simultaneously, then, the facility needs to be fully shut down every TI. In case parallel testing is not chosen for any subsystem, OP may be chosen as a multiple of TI. Fig. 7 shows an example of the time horizon with $OP = 2 \cdot TI$. The duration of the downtime during the overhaul is determined in (16).

The probabilities of the technological solution being in particular states of the Markov model over time are described by a set of ODEs in (17). The non-zero transition rates are provided in (18). The starting

Table 3
States of the Markov model[a].
Source: Redutskiy [5,6]

#	T	LS	FCE	Tech	Comments
1	Up	Up	Up	Up	Normal course of the process
2	Up	Up	Up	Down	ESD has performed its function
3	O/S	Up	Up	Down	overhaul after a spurious trip
4	Up	O/S	Up	Down	Overhaul after a spurious trip
5	Up	Up	O/S	Down	Overhaul after a spurious trip
6	O/D	Up	Up	Down	overhaul after a dangerous failure
7	Up	O/D	Up	Down	Overhaul after a dangerous failure
8	Up	Up	O/D	Down	Overhaul after a dangerous failure
9	Failure	Up	Up	Up	Dangerous undetected failure
10	Up	Failure	Up	Up	Dangerous undetected failure
11	Up	Up	Failure	Up	Dangerous undetected failure
12	ESD is in the downstate, incident has occurred				Failure-on-demand state

[a]Here, the following notations are used: T — subsystem of transmitters, LS — logic solvers, FCE — final control elements, Tech — technology.

Table 4
Notations for the lifecycle model.

Indices and parameters	
i, j	Indices for the Markov model states
q	Index for the diverse-redundant subsystems of the SIS; $q = \{1, 2, 3\}$ correspond to sensors, PLCs, and actuators
k	Index for the time intervals the lifecycle is split into
K	Total number of periods the lifecycle is split into
TI	Test interval, h
OP	Overhaul period which has to be a multiple of TI, h
LC_h	Duration of the lifecycle, h
T^{SU}	Start-up time for the technology after the shutdown, h
T_q^{TR}	Test & repair time for one device in subsystem q, h
T^{OD}	Downtime due to SIS and/or technology overhaul, h
$x_{q,p}^{TP}$	Binary indicator: equals 1 if testing policy p is chosen for subsystem q; $p = \{1, 2, 3\}$ correspond to parallel, sequential, and staggered testing
N_q	Total number of devices in subsystem q
$\lambda_{i,j}$	Transition rate from state i to state j, h^{-1}
λ_q^{DU}	Dangerous undetected failure rate for the qth subsystem, h^{-1}
λ_q^{DD}	Dangerous detected failure rate for the qth subsystem, h^{-1}
λ_q^{ST}	Spurious tripping rate for the qth subsystem, h^{-1}
r	Incidents occurrence rate, h^{-1}
μ^t	Restoration rate for the technology, h^{-1}
π_j^k	Initial condition (probability of each jth state) for the kth time interval of the planning horizon
Variables	
$p_j(t)$	Probability of the process being in the jth state
Outputs of the model	
PFD_{avg}	Average probability of failure on demand
DT	Mean down time of the process, h

point of the stochastic process at $t = 0$ is State 1 (19). Initial probabilities at the start of every time interval defined in (15) are provided in (20). The logic behind this reassignment of the probability values at the junction of the intervals of this switching Markov process is that the undetected failures in all the SIS's subsystems become fully resolved after the overhauls. Thus, the probabilities of states 9–12 are set to zero.

The solution of the ODEs is used to evaluate the two safety-related indicators for the decision-making framework in Fig. 4. The average probability of failure on demand is calculated based on the probability of the process being in state 12, while the expected facility downtime is calculated given the probability values for states 2–8, as demonstrated in (21).

$$K = \left\lceil \frac{LC_h}{OP} \right\rceil,$$
$$t \in [0; OP] \cup [OP + T^{OD}; 2 \cdot OP] \cup \cdots \cup [(K-1) \cdot OP + T^{OD}; k \cdot OP]. \tag{15}$$

$$T^{OD} = \max_q \left(x_{q,1}^{TP} \cdot T_q^{repair} + x_{q,2}^{TP} \cdot N_q \cdot T_q^{repair} + x_{q,3}^{TP} \cdot 0 \right) + T^{SU} \tag{16}$$

$$\frac{dp_j(t)}{dt} = \sum_{i=1}^{12} p_i(t) \cdot \lambda_{i,j}, \quad j \in \{1, \dots, 12\} \tag{17}$$

$$\begin{aligned}
&\lambda_{1,1} = -\left(\sum_q \lambda_q^{ST} + \sum_q \lambda_q^{DD} + \sum_q \lambda_q^{DU} + r \right), \quad \lambda_{1,2} = r, \quad \lambda_{1,3} = \lambda_1^{ST}, \\
&\lambda_{1,4} = \lambda_2^{ST}, \quad \lambda_{1,5} = \lambda_3^{ST}, \\
&\lambda_{1,6} = \lambda_1^{DD}, \quad \lambda_{1,7} = \lambda_2^{DD}, \quad \lambda_{1,8} = \lambda_3^{DD}, \quad \lambda_{1,9} = \lambda_1^{DU}, \quad \lambda_{1,10} = \lambda_2^{DU}, \\
&\lambda_{1,11} = \lambda_3^{DU}, \quad \lambda_{2,1} = \mu^t, \\
&\lambda_{2,2} = -\mu^t, \quad \lambda_{3,1} = \mu, \quad \lambda_{3,3} = -\mu, \quad \lambda_{4,1} = \mu, \quad \lambda_{4,4} = -\mu, \quad \lambda_{5,1} = \mu, \\
&\lambda_{5,5} = -\mu, \quad \lambda_{6,1} = \mu, \\
&\lambda_{6,6} = -\mu, \quad \lambda_{7,1} = \mu, \quad \lambda_{7,7} = -\mu, \quad \lambda_{8,1} = \mu, \quad \lambda_{8,8} = -\mu, \quad \lambda_{9,4} = \lambda_2^{ST}, \\
&\lambda_{9,5} = \lambda_3^{ST}, \quad \lambda_{9,7} = \lambda_2^{DD}, \\
&\lambda_{9,8} = \lambda_3^{DD}, \quad \lambda_{9,9} = -\left(\lambda_2^{ST} + \lambda_3^{ST} + \lambda_2^{DD} + \lambda_3^{DD} + r\right), \quad \lambda_{9,12} = r, \\
&\lambda_{10,3} = \lambda_1^{ST}, \quad \lambda_{10,5} = \lambda_3^{ST}, \\
&\lambda_{10,6} = \lambda_1^{DD}, \quad \lambda_{10,8} = \lambda_3^{DD}, \quad \lambda_{10,10} = -\left(\lambda_1^{ST} + \lambda_3^{ST} + \lambda_1^{DD} + \lambda_3^{DD} + r\right), \\
&\lambda_{10,12} = r, \quad \lambda_{11,3} = \lambda_1^{ST}, \\
&\lambda_{11,4} = \lambda_2^{ST}, \quad \lambda_{11,6} = \lambda_1^{DD}, \quad \lambda_{11,7} = \lambda_2^{DD}, \\
&\lambda_{11,11} = -\left(\lambda_1^{ST} + \lambda_2^{ST} + \lambda_1^{DD} + \lambda_2^{DD} + r\right), \quad \lambda_{11,12} = r.
\end{aligned} \tag{18}$$

$$\pi_1^1 = 1, \quad \pi_2^1 = 0, \quad \cdots \quad \pi_{12}^1 = 0. \tag{19}$$

$$\begin{aligned}
\pi_1^k &= p_1\big((k-1)\cdot OP\big) + p_9\big((k-1)\cdot OP\big) + p_{10}\big((k-1)\cdot OP\big) \\
&\quad + p_{11}\big((k-1)\cdot OP\big) + p_{12}\big((k-1)\cdot OP\big); \\
\pi_j^k &= p_j\big((k-1)\cdot OP\big), \quad j \in \{2,3,4,5,6,7,8\}; \\
\pi_j^k &= 0, \quad j \in \{9,10,11,12\}, \\
&\quad k \in \{2, \dots, K\}.
\end{aligned} \tag{20}$$

$$\begin{aligned}
PFD_{avg} &= \frac{1}{LC_h} \cdot \int_0^{LC_h} PFD(t)dt = \frac{1}{OP} \cdot \int_0^{OP} p_{12}(t)dt \\
&\quad + \sum_{k=2}^{K} \frac{1}{OP - T^{OD}} \cdot \int_{(k-1)\cdot OP + T^{OD}}^{k\cdot OP} p_{12}(t)dt; \\
DT &= \sum_{j=2}^{8} \int_0^{LC_h} p_j(t)dt.
\end{aligned} \tag{21}$$

3.4. Employee scheduling model

This section presents two blocks in the modeling framework depicted in Fig. 4, namely "Staffing size evaluation" and "Employee scheduling". The former one is used to compute the requirements to the maintenance personnel to be present at the facility during every week of one-year planning horizon (for further purposes of employee scheduling). The second modeling block solves the employee scheduling problem itself.

Table 5 contains the notations necessary to describe these modeling blocks.

To determine the requirement to the maintenance staff size, the two kinds of maintenance – continuous and periodic – have to be considered separately. For the continuous maintenance, the personnel requirement is calculated based on the architectural choices for each subsystem, as well as the time limit imposed on resolving the detected device failures (DD and ST), as demonstrated in (22). Further, the demand for personnel for the parallel and sequential periodic tests is calculated in (23), again, based on the subsystems' architectures. Expression (24) describes the personnel requirements for the cases when staggered proof-testing is chosen for certain subsystems. To sum up, the total demand for the number of employees required to be present at the remote facility at any given week of the one-year planning horizon is demonstrated in (25).

Table 5
Notations for the employee scheduling model.

Notation	Description
Indices and sets	
w	Index for weeks in one-year planning horizon: $w \in \{1, \dots, 52\}$
q	Index for the MooN architectures the SIS comprises (each MooN architecture among the diverse-redundant structures is enumerated)
r	Index for redundancy alternatives
l	Index for trips
s	Index for daily schedule alternatives: 8-hour daily work or 12-hour daily schedule
p	Index for proof testing policies: $p = \{1, 2, 3\}$ corresponding to parallel, sequential, and staggered testing policies
S_q^{red}	Set of redundancy architecture alternatives for the qth MooN redundancy architecture
S^{trip}	Set of trips (all possible trip start times and durations of one, two, four, or six weeks)
$S^{4w.trip}$	Set of all possible 4-week trips
S^{sched}	Set of alternative daily work schedules (work–rest schedule during each day)
Parameters	
$N_{r,q}$	The total number of devices in the qth MooN architecture given the redundancy option r
$M_{r,q}$	The number of devices in qth MooN architecture required to be operating given its redundancy r
$x_{r,q}^{red}$	Binary indicator signaling which redundancy option r is chosen for the qth MooN redundancy architecture
T_q^{TR}	Test & repair time of the devices in the qth MooN redundancy architecture
$T^{TR.max}$	The upper bound on the test & repair time for the entire SIS for continuous maintenance (8 h)
$\sigma_{l,w}$	A binary parameter indicating whether week w is covered by the trip option l or not
S_s^{crew}	Crew size associated with any particular daily work schedule alternative s
β_s^{sched}	Employee pay rate cost modifier given the chosen daily schedule alternative s
$x_{q,p}^{TP}$	Binary indicator: equals 1 if testing policy p is chosen for the qth MooN redundancy architecture
$d_w^{continuous}$	Weekly demand for the employees for continuous maintenance
$d_w^{periodic}$	Weekly demand for the employees for periodic parallel or sequential proof tests
$d_{w,q}^{staggered}$	Weekly demand for the employees for periodic staggered proof tests for the qth MooN redundancy architecture
d_w^{emp}	Total demand for the number of workers whose presence is required at the facility during week w
$C^{WF.est}$	Initial investments associated with establishing local workforce
$C^{WF.oper}$	Yearly operational expenditures associated with the local workforce
C^{start}	Subsidiary start-up cost
C^{train}	Cost of training one maintenance engineer
C^{comp}	Yearly expenditures associated with running the local subsidiary
C^{wage}	Average monthly salary of one maintenance engineer
C_l^{trip}	Cost of one worker's trip to the remote location and back depending on the trip duration
Decision variables	
$y_{l,s}^{travel}$	Integer variable: number of service crews taking trip l to travel to the facility and work according to daily schedule s

The employee scheduling modeling block begins with evaluating the workforce-related costs distinguishing capital and operational expenditures. Initial investments are expressed in (26) and they include start-up cost of opening a local subsidiary company and training the engineers to perform maintenance for the oil and gas facilities. Annual operating costs related to the workforce are given in (27). The expression describes costs related to running the company, the employee salaries as well as the costs of traveling to the remote locations and back. The second term in (26) and in (27) roughly evaluates the staff size required for the company to hire. The number of employees to be hired is evaluated by calculating the collective effort expressed in "people-weeks" which is further divided by the maximum time the employees are supposed to spend in trips to the remote locations.

Expression (28) represents the set-covering constraint ensuring that the demand for the employees is satisfied during any given week. The

extension of the Dantzig's formulation here is done by introducing the choice between the daily schedules: either 8h working day (which requires three people in the maintenance crew) or 12h working day (two people in the crew).

$$d_w^{continuous} = \left\lceil \sum_q \left(\sum_{r \in S_q^{red}} N_{r,q} \cdot x_{r,q}^{red} - \sum_{r \in S_q^{red}} M_{r,q} \cdot x_{r,q}^{red} \right) \cdot \frac{T_q^{TR}}{T^{TR.max}} \right\rceil, \quad w = \{1, \dots, 52\} \setminus \left\{ \frac{TI}{7 \cdot 24}; \frac{2 \cdot TI}{7 \cdot 24}; \frac{3 \cdot TI}{7 \cdot 24}; \dots; 52 \right\}. \tag{22}$$

$$d_w^{periodic} = \sum_q \left(x_{q,1}^{TP} \cdot \sum_{r \in S_q^{red}} N_{r,q} \cdot x_{r,q}^{red} + x_{q,2}^{TP} \cdot 1 \right), \quad w = \left\{ \frac{TI}{7 \cdot 24}; \frac{2 \cdot TI}{7 \cdot 24}; \frac{3 \cdot TI}{7 \cdot 24}; \dots; 52 \right\}. \tag{23}$$

$$d_w^{staggered} = x_{q,3}^{TP} \cdot 1, \quad w = \left\{ \frac{TI}{7 \cdot 24 \cdot \sum_{r \in S_q^{red}} N_{r,q} \cdot x_{r,q}^{red}} \cdot \frac{1}{2}; \frac{TI}{7 \cdot 24 \cdot \sum_{r \in S_q^{red}} N_{r,q} \cdot x_{r,q}^{red}} \cdot \frac{3}{2}; \dots; 52 \right\}, \forall q. \tag{24}$$

$$d_w^{emp} = d_w^{continuous} + d_w^{periodic} + \sum_q d_w^{staggered}, \quad \forall w. \tag{25}$$

$$C^{WF.est} = C^{start} + C^{train} \cdot \sum_{w=1}^{52} \sum_{l \in S^{trip}} \sum_{s \in S^{sched}} \frac{S_s^{crew} \cdot \sigma_{l,w}}{T^{trip.max}} \cdot y_{l,s}^{travel} \tag{26}$$

$$C^{WF.oper} = C^{comp} + 12 \cdot C^{wage} \sum_{l \in S^{trip}} \sum_{s \in S^{sched}} \frac{S_s^{crew} \cdot \sigma_{l,w}}{T^{trip.max}} \cdot y_{l,s}^{travel} + \sum_{l \in S^{trips}} \sum_{s \in S^{sched}} C_l^{trip} \cdot \beta_s^{crew} \cdot S_s^{crew} \cdot y_{l,s}^{travel} \tag{27}$$

$$\sum_{l \in S^{trips}} \sum_{s \in S^{sched}} \sigma_{l,w} \cdot y_{l,s}^{travel} \geq d_w^{emp}, \quad \forall w \in \{1, \dots, 52\}. \tag{28}$$

3.5. Lifecycle modeling from the economic perspective

Lifecycle of the SIS solutions operating for particular hazardous technologies in the oil and gas sector lasts many years. Therefore, to create a reasonable representation of the expenditures through the solution's lifecycle, the following three major cost components are considered. First, procurement costs, or, in other words, capital investments. These are the costs of initiating the project, starting the system design project, preparing the necessary documentation, equipment, as well as organizing and training staff. Second, annual operational costs: these costs include the use of electric energy by the system's instrumentation, costs of conducting continuous and periodic maintenance, as well as production losses due to downtime. For the SIS solutions in remote locations, it is also relevant to consider annual costs of employee scheduling (maintenance crews traveling to remote locations to perform diagnostics). And finally, annual risk costs include the expected values of losses the operating company has to bear in case an incident occurs and hazardous consequences take place. Also, in part, these costs include the negative impact that any SIS brings to a facility which comes in a form of unwanted shutdowns (spurious trips), which, in turn, leads to downtime and production losses.

Table 6 contains the notations that are necessary to describe these cost components.

First of all, the general lifecycle approach to evaluating the cost of the solution is demonstrated in (29) as the present value of the lifecycle costs. The capital (procurement) investments are elaborated in (30). Here, the first term shows the costs of the project initiation and designing an SIS. The second term corresponds to the costs of purchasing the instrumentation. Finally, the third term shows the costs of establishing the local company and the local engineering staff, which has previously been explained in (26).

The details of the annual operations cost are provided in (31). The first term here refers to the electrical energy consumption by the instrumentation. The second term corresponds to the expenditures associated with periodic proof testing conducted with a chosen period TI. The next term expresses the expected losses associated with facility downtime due to dangerous failures of the entire safety instrumented system. The next term stands for the yearly costs of mandatory maintenance of the technological units. The following term describes the losses due downtime related to facility overhauls. The last term included into the operational costs describes the yearly employee scheduling expenditures explained earlier in (27). Formula (32) shows the costs associated with spare parts replenishment. The spare parts are used during the maintenance, and therefore, the stock has to be filled up to the necessary level regularly.

Annual risk costs are evaluated in (33). The expression covers the expected production losses due to the facility downtime cause by spurious tripping of the entire safety system, and also the expected losses (or costs of residual risk of incidents) if an unwanted turn of events takes place and the company has to deal with the hazardous consequences.

Expression (31) utilizes the yearly value of the dangerous detected failure rate of the entire safety system. Also, expression (33) utilizes

Table 6
Notations for the employee scheduling model.

Notation	Description
q	Index of the redundant architecture of the SIS's subsystems
τ	Time, y
r	Index for redundancy alternatives in the set S_q^{red} defined for each qth MooN redundancy block
l	Index for instrumentation alternatives in the set S_q^{inst} defined for each qth MooN redundancy block
$N_{r,q}$	The total number of devices in the qth MooN architecture given the redundancy option r
$x_{r,q}^{red}$	Binary indicator signaling which redundancy option r is chosen for the qth MooN redundancy block
$x_{l,q}^{inst}$	Binary indicator signaling which instrumentation option l is chosen for the qth MooN redundancy block
x_q^{sep}	Binary indicator signaling which separation option is chosen for the qth MooN block (baseline or additional separation)
β_q^{design}	Design cost modifier for block q chosen among the options $\beta_q^{design1}$ and $\beta_q^{design2}$ based on the choice of electrical separation
β_q^{purch}	Purchase cost modifier for block q chosen among the options β_q^{purch1} and β_q^{purch2} based on the choice of electrical separation
β_q^{cons}	Consumption cost modifier for block q chosen among the options β_q^{cons1} and β_q^{cons2} based on the choice of electrical separation
$C^{lifecycle}$	Lifecycle cost, currency units (CU)[a]
$C^{procurement}$	Procurement cost, CU
$C_\tau^{operations}$	Yearly operation cost, CU
C_τ^{risk}	Yearly risk cost, CU
C^{design}	Design cost, CU
$C^{WF.est}$	Cost of establishing the workforce, CU
C_q^{purch}	Cost of purchasing one device chosen for the qth MooN redundancy block, CU
C_q^{cons}	Yearly electricity consumption by one device in the qth MooN redundancy block, CU
C_q^{test}	Cost of conducting one proof test for one component of the qth MooN redundancy block, CU
C_q^{repair}	Cost of repairing one component of the qth MooN redundancy block, CU
C_q^{SP}	Cost of spare parts replenishment for the qth MooN redundancy block, CU
C^{PL}	Hourly losses of production, CU/h
C^{FM}	Yearly cost of facility maintenance, CU
$C^{WF.oper}$	Operational expenses associated with the workforce: travels, salaries, bonuses, etc., CU
C^{inc}	Cost of an incident and hazardous consequences, CU
φ	Spare part cost fraction
LC_y	Lifecycle duration, y
T^{OD}	Start-up time after the shutdown necessary for maintenance before the facility can be restarted, h
DDR_y	Dangerous detected failure rate for the given ESD, y^{-1}
STR_y	Spurious tripping rate for the given ESD, y^{-1}

[a]In this research, fictional currency units (CU) are used to mask the real purchase costs in the device database provided in the next section of the paper. It is done so that particular instrumentation vendors would not be identifiable.

Table 7
Data for the model. Shutdown procedure description.

Critical process parameters				Shutdown actions		
#	Process parameter	Event	Frequency, y^{-1}	#	Final control element	Action
1	Liquid level in the tank	Level ⩾ HH	0.075	1	Safety Valve 1 on the fill line	Close
2	Fire in the tank	Fire detected	0.03	2	Safety Valve 2 on the output line	Close
				3	Pump delivering oil to the tank	Shutdown

Table 8
Modeling parameters and equipment database.

Instrumentation alternatives: part 1													
Alternative	Smart level sensors:				Standard level sensors:			Level switches:			Fire detectors:		
	sLT1	sLT2	sLT3	sLT4	LT1	LT2	LT3	LS1	LS2	LS3	FD1	FD2	FD3
Failure rate, $\times 10^{-6}$ h^{-1}													
Dangerous failures	2	7.1	0.3	0.7	2	0.58	20	20	8	10	20	6	1.2
Spurious trips	1.5	3	0.12	0.5	1	4	10	15	5	6.5	10	4	2.28
Diagnostic coverage, %	67	50	85	90	67	40	60	50	60	50	0	35	40
Costs													
Purchase, CU[a]	1700	2500	2500	3000	1400	1750	850	400	500	500	40	57.5	85
Design, CU	120	170	100	150	5	5	6	5	5	5	5	5	5
Consumption, CU	1.5	6	1	5	1.5	0.5	1	1	1	1	0.5	0.5	0.5
Repair, CU	3	12	5	8	5	2.5	2	2	2	2	2	2	2
Test, CU/event	10	5	12	5	5	4	5	2	2	2	3	3	3
Redundancy alternatives	1oo1, 1oo2, 1oo3, 1oo4, 2oo2 2oo3				1oo1, 1oo2, 1oo3, 1oo4, 2oo2, 2oo3			1oo1, 1oo2, 1oo3, 1oo4			2oo2, 2oo3, 2oo4, 2oo5, 2oo6, 2oo7, 2oo8		

Instrumentation alternatives: part 2												
Alternative	PLCs/logic solvers:			Smart valves:		Standard safety valves:			Smart drives:		Standard pump drives:	
	PLC1	PLC2	PLC3	sSV1	sSV2	SV1	SV2	SV3	sPD1	sPD2	PD1	PD2
Failure rate, $\times 10^{-6}$ h^{-1}												
Dangerous failures	0.9	1.3	5.9	0.36	0.5	67	40	90	0.1	0.2	27	17
Spurious trips	0.8	1.1	5.5	0.18	0.1	33	33	30	0.15	0.09	13	9
Diagnostic coverage, %	90	98	97	75	67	20	30	10	70	75	20	30
Costs												
Purchase, CU	22500	12500	7500	3500	3000	1300	1750	1400	4000	4500	750	1250
Design, CU	2000	1000	600	900	1000	650	900	900	1000	1000	100	100
Consumption, CU	500	500	400	400	500	250	200	100	500	600	50	75
Repair, CU	1000	1000	750	100	800	500	500	500	100	120	75	100
Test, CU/event	5	5	5	80	50	45	40	25	100	80	50	40
Redundancy alternatives	1oo1, 1oo2, 1oo3, 1oo4, 2oo3			1oo1, 1oo2, 1oo3, 1oo4		1oo1, 1oo2, 1oo3, 1oo4			1oo1, 1oo2 1oo3		1oo1, 1oo2, 1oo3	

Common cause failure				
CCF factor for all subsystems		Cost modifier	Baseline solution	Electrical separation
Baseline solution (standard circuits)	0.035	Purchase cost	1	1.35
Additional electrical separation	0.020	Design cost	1	1.10
		Consumption cost	1	1.35

Other parameters	
Repair rate for the subsystems: $\mu = 0.125$ h^{-1}	Cost of hazard: 50 000 000 CU
Facility restoration rate: $\mu^{t} = 0.0625$ h^{-1}	Start-up cost: 10 000 000 CU
Lifecycle duration: $LC_y = 15$ y	Production loss: 1 000 CU/h
TI is chosen from a set of integer values between 12 and 52 weeks.	Discount rate: $\delta = 5\%$

the yearly spurious tripping rate for the entire SIS. These values are explained in (34) as they are based on the outcome of the Markov model for the SIS lifecycle presented in Section 3.3 of this paper.

Formulas (30) and (31) contain several cost modifiers that assume different values depending on the choice of additional separation of the devices within the subsystems (values of β for design, purchasing and electricity consumption). Eqs. (35) demonstrate this choice.

$$C^{lifecycle} = C^{procurement} + \sum_{\tau=1}^{LC_y} \left(C_{\tau}^{operations} + Cost_{\tau}^{risk}\right) \cdot \frac{1}{(1+\delta)^{\tau-1}} \tag{29}$$

$$C^{procurement} = C^{design} \cdot \beta^{design} + \sum_{q} \sum_{l \in S_q^{inst}} \sum_{r \in S_q^{red}} C_{l,q}^{purch} \cdot x_{l,q}^{inst} \cdot \beta^{purch} \cdot N_{r,q} \cdot x_{r,q}^{red} + C^{WF.est} \tag{30}$$

$$\begin{aligned} C_{\tau}^{operations} = & \sum_{q} \sum_{l \in S_q^{inst}} \sum_{r \in S_q^{red}} C_{l,q}^{cons} \cdot x_{l,q}^{inst} \cdot \beta^{cons} \cdot N_{r,q} \cdot x_{r,q}^{red} \\ & + \frac{52 \cdot 7 \cdot 24}{TI} \cdot \sum_{q} \sum_{l \in S_q^{inst}} \sum_{r \in S_q^{red}} C_{l,q}^{test} \cdot x_{l,q}^{inst} \cdot N_{r,q} \cdot x_{r,q}^{red} \\ & + \left(C^{PL} \cdot T^{SU} + \sum_{q} \sum_{l \in S_q^{inst}} \sum_{r \in S_q^{red}} C_{l,q}^{rep} \cdot x_{l,q}^{inst} \cdot N_{r,q} \cdot x_{r,q}^{red} + \sum_{q} C_{q}^{SP} \right) \cdot DDR_y \\ & + C^{FM} + \frac{52 \cdot 7 \cdot 24}{OP} \cdot C^{PL} \cdot T^{OD} + C^{WF.oper} \end{aligned} \tag{31}$$

$$C_{q}^{SP} = \varphi \cdot \sum_{q} \sum_{l \in S_q^{inst}} \sum_{r \in S_q^{red}} C_{l,q}^{purch} \cdot x_{l,q}^{inst} \cdot \beta^{purch} \cdot N_{r,q} \cdot x_{r,q}^{red} \tag{32}$$

$$C_{\tau}^{risk} = \left(C^{PL} \cdot T^{SU} + \sum_{q} \sum_{l \in S_q^{inst}} \sum_{r \in S_q^{red}} C_{l,q}^{rep} \cdot x_{l,q}^{inst} \cdot N_{r,q} \cdot x_{r,q}^{red} \right) \cdot STR_y + C^{inc} \cdot r \cdot PFD_{avg} \tag{33}$$

$$DDR_y = -52 \cdot 7 \cdot 24 \cdot \frac{\log\left(1 - \sum_{j=6}^{8} p_j\left(LC_h\right)\Big|_{X^{inst}, X^{red}, X^{sep}, TI, OP}\right)}{LC_h}$$
$$STR_y = -52 \cdot 7 \cdot 24 \cdot \frac{\log\left(1 - \sum_{j=3}^{5} p_j\left(LC_h\right)\Big|_{X^{inst}, X^{red}, X^{sep}, TI, OP}\right)}{LC_h} \tag{34}$$

$$\beta_q^{design} = \beta^{design1} \cdot \left(1 - x_q^{sep}\right) + \beta^{design2} \cdot x_q^{sep},$$
$$\beta_q^{purch} = \beta^{purch1} \cdot \left(1 - x_q^{sep}\right) + \beta^{purch2} \cdot x_q^{sep}, \tag{35}$$
$$\beta_q^{cons} = \beta^{cons1} \cdot \left(1 - x_q^{sep}\right) + \beta^{cons2} \cdot x_q^{sep}, \quad \forall q.$$

4. Computational experiment

4.1. Experiment setting and optimization algorithm

The data for the computational experiment to test the suggested decision-making framework have been procured from a petroleum company operating remotely-located facilities in Russia. The facility considered for this case is a depot for the storage of unprocessed fluid hydrocarbons. This depot is intended for temporary storage (up to a few days) of the fluid delivered from an oilfield when the capacity of the main petroleum processing facility is exceeded or in case an emergency situation at that facility.

Possible critical situations that may occur at the storage depot as well as the required shutdown measures are described in Table 7. For the subsystem of level sensors, standard devices, smart devices, and switches are possible. For the fire detector subsystem, only standard devices are available. For the safety valves, both smart and standard device alternatives have been considered during the technological solution design. The reliability block-diagram representation of an ESD system for this technological unit matches the one provided in Fig. 1e comprising 11 MooN blocks. All the instrumentation alternatives considered by the engineering contractor for this project are provided in Table 8 together with their reliability characteristics and costs.

In addition to the safety perspective on the engineering solution design, this research addresses the issue of employee scheduling for conducting maintenance on the remotely-located facility. Therefore, the data regarding typical trip durations, daily schedules, and respective compensations have been collected from the E&P operator owning this facility. These data are presented in Table 9.

The overall decision-making framework (Fig. 4) has been implemented in MATLAB where the solver `gamultiobj` (multi-objective genetic algorithm, a variant of NSGA-II) optimized the black-box modeling framework programmed as a script-function. For the details of the applied heuristic algorithm, Mathworks refers the users to Deb [34]. For the considered example, the problem includes 148 variables, of which 146 are binaries and the remaining two are integers. The following settings for the solver are applied: population size: 300; initial population created with the uniform distribution applying a customized function suggested by Mathworks; selection function: tournament; generational gap: 0.8 (or 80%); crossover and mutation functions: customized functions suggested by Mathworks.

The script-function has been programmed in such a way that certain constraints are fulfilled implicitly. These are logical constraints implying that for each redundant block of the designed SIS, only one device model, only one redundancy alternative, only one separation option, and only one proof testing policy must be chosen. Additional constraints have been enforced with the help of penalty terms to the lifecycle cost. One type of such constraints is the SIL3 requirements (the upper bound on PFD_{avg} and architectural prerequisites) expressed in Table 1. Another constraint enforces a certain specification on the level sensor subsystem stating that at least one continuous-value transmitter (either standard or smart) must be used. Yet another constraint ensures that periodic overhauls are conducted at least once a year.

Table 9
Trips and daily schedules with associated costs.

Daily work schedule alternatives			
#	Description	# of workers for continuous service	Pay rate, [CU/day]
1	8 h of work, 16 h of rest	3	125
2	12 h of work, 12 h of rest	2	250
Daily work schedule alternatives			
#	Description	Pay rate cost modifier	
1	1-week trip	1	
2	2-week trip	1.25	
3	4-week trip	1.5	
4	6-week trip	2	

4.2. Results and discussion

When the results of the optimization run have been produced, the SIS design specifications and maintenance-related decisions in the Pareto-front solutions may be studied to help reveal certain preferences for the solution under design. These tendencies the produced solutions exhibit may help formulate the requirements specification for the SIS in a clear way so that adequate groundwork would be laid for the further detailed design of the SIS.

The results presented in Tables 10 and 11 are studied and certain observations are made.

- The optimization algorithm clearly prefers field devices (sensors and actuators) with better reliability characteristics despite the higher purchase costs associated with them.
- For the overwhelming majority of the architectures in the produced results, adding electrical separation is preferred.
- The diverse redundancy is always chosen for the subsystems where it is allowed. One may also observe that at least two devices of each device type allowed for the diverse-redundant architectures are chosen. The results show that diversity is clearly preferred over homogeneousness within the subsystem's architectures. The advantages of introducing diversity into most subsystems are also evident from the reliability indicators computed for the produced solutions in Table 11.
- For the level sensors, device models sLT3 and LT2 are mostly chosen for continuous level measurements, while device model LS2 is chosen for switches. For standard and smart sensors, architecture 1oo3 is generally preferred, however, for some solutions, 1oo2 and 1oo4 are chosen. For the level switches, architecture 1oo4 is preferred.
- The highest possible redundancy 2oo8 is selected for the fire detectors. It may be attributed to the comparatively low cost of these devices. Device model FD3 is always chosen. Of the available device alternatives for fire detectors, this model has the highest purchase cost and the best reliability characteristics.
- For the subsystem of PLCs, device model PLC2 is chosen with the architecture 1oo3 for all solutions.
- For the actuator subsystems, the smart valves sSV1 and standard valve SV2 are chosen most often. Their preferred architectures are 1oo2 and 1oo3. It is clear from the produced results (solution 1 specification in Table 10 and reliability characteristics in Table 11) that it is possible to achieve SIL3 with 1oo2 architecture for safety valves.
- For the smart pump drive subsystem, device model sPD1 is mostly chosen with the architecture 1oo2. For the ordinary pump drives, PD2 is always chosen with 1oo2 architecture.

Table 10
Specification for the Pareto-front solutions.

#	Level sensors			Fire detector	PLC	Actuators: Safety Valve 1	
	Smart	Standard	Switch			Smart	Standard
1	1oo3/e/sLT3 Sequential	1oo4/e/LT2 Sequential	1oo4/e/LS2 Staggered	2oo8/e/FD3 Sequential	1oo3/e/PLC2 Sequential	1oo2/e/sSV2 Staggered	1oo2/e/SV2 Staggered
2	1oo3/e/sLT3 Staggered	1oo3/e/LT2 Staggered	1oo4/e/LS2 Staggered	2oo8/e/FD3 Staggered	1oo3/e/PLC2 Staggered	1oo2/e/sSV2 Staggered	1oo2/e/SV2 Staggered
3	1oo3/e/sLT3 Staggered	1oo4/e/LT2 Staggered	1oo3/e/LS2 Staggered	2oo8/e/FD3 Staggered	1oo3/e/PLC2 Staggered	1oo2/e/sSV1 Staggered	1oo2/e/SV2 Staggered
4	1oo3/e/sLT3 Staggered	1oo3/e/LT3 Staggered	1oo4/e/LS2 Staggered	2oo8/e/FD3 Sequential	1oo3/e/PLC2 Sequential	1oo2/e/sSV2 Staggered	1oo3/e/SV2 Staggered
5	1oo3/e/sLT3 Sequential	1oo3/e/LT3 Sequential	1oo4/e/LS2 Sequential	2oo8/e/FD3 Sequential	1oo3/e/PLC2 Sequential	1oo3/e/sSV1 Sequential	1oo2/e/SV2 Staggered
6	1oo3/e/sLT3 Sequential	1oo3/e/LT3 Sequential	1oo4/e/LS2 Sequential	2oo8/e/FD3 Staggered	1oo3/e/PLC2 Sequential	1oo3/e/sSV1 Sequential	1oo2/e/SV2 Staggered
7	1oo3/e/sLT3 Sequential	1oo2/e/LT2 Sequential	1oo4/e/LS2 Sequential	2oo8/e/FD3 Sequential	1oo3/e/PLC2 Sequential	1oo3/e/sSV2 Staggered	1oo2/e/SV2 Staggered
8	1oo3/e/sLT3 Sequential	1oo3/e/LT2 Sequential	1oo4/b/LS2 Sequential	2oo8/e/FD3 Sequential	1oo3/e/PLC2 Sequential	1oo2/e/sSV1 Staggered	1oo3/e/SV2 Staggered
9	1oo3/e/sLT3 Sequential	1oo2/e/LT2 Sequential	1oo4/e/LS2 Sequential	2oo8/e/FD3 Sequential	1oo3/e/PLC2 Sequential	1oo3/e/sSV1 Staggered	1oo3/e/SV2 Staggered
10	1oo3/e/sLT3 Sequential	1oo3/e/LT2 Sequential	1oo4/e/LS2 Sequential	2oo8/e/FD3 Sequential	1oo3/e/PLC2 Sequential	1oo3/e/sSV1 Staggered	1oo2/e/SV2 Staggered
11	1oo3/e/sLT3 Sequential	1oo3/e/LT2 Sequential	1oo4/e/LS2 Sequential	2oo8/e/FD3 Sequential	1oo3/e/PLC2 Sequential	1oo3/e/sSV1 Staggered	1oo3/e/SV2 Staggered
12	1oo3/e/sLT3 Staggered	1oo3/e/LT2 Sequential	1oo4/e/LS2 Sequential	2oo8/e/FD3 Sequential	1oo3/e/PLC2 Sequential	1oo3/e/sSV1 Staggered	1oo2/e/SV2 Staggered

#	Actuators: Safety Valve 2		Actuators: Pump drive		Test interval,	Overhaul period,	Staff size
	Smart	Standard	Smart	Standard	Weeks	Weeks	
1	1oo2/e/sSV2 Staggered	1oo2/e/SV2 Staggered	1oo2/e/sPD2 Staggered	1oo2/e/PD2 Staggered	52	52	28
2	1oo2/e/sSV1 Staggered	1oo2/e/SV2 Staggered	1oo2/e/sPD2 Staggered	1oo2/b/PD2 Staggered	52	52	28
3	1oo2/e/sSV1 Staggered	1oo2/e/SV2 Staggered	1oo2/e/sPD2 Staggered	1oo2/e/PD2 Staggered	52	52	28
4	1oo2/e/sSV2 Staggered	1oo2/e/SV2 Staggered	1oo2/e/sPD2 Staggered	1oo2/e/PD2 Sequential	48	48	32
5	1oo2/e/sSV2 Staggered	1oo2/e/SV2 Staggered	1oo2/e/sPD2 Sequential	1oo2/e/PD2 Sequential	24	48	32
6	1oo2/e/sSV1 Staggered	1oo2/e/SV2 Staggered	1oo2/e/sPD2 Sequential	1oo2/e/PD2 Sequential	24	48	33
7	1oo2/e/sSV2 Sequential	1oo2/e/SV2 Staggered	1oo2/e/sPD1 Sequential	1oo2/e/PD2 Sequential	16	48	28
8	1oo2/e/sSV1 Staggered	1oo2/e/SV2 Staggered	1oo2/e/sPD2 Sequential	1oo2/e/PD2 Sequential	16	48	34
9	1oo2/e/sSV1 Staggered	1oo2/e/SV2 Staggered	1oo2/e/sPD2 Sequential	1oo2/e/PD2 Sequential	16	48	34
10	1oo2/e/sSV1 Staggered	1oo2/e/SV2 Sequential	1oo2/e/sPD2 Sequential	1oo2/e/PD2 Sequential	16	48	33
11	1oo2/e/sSV1 Staggered	1oo2/e/SV2 Staggered	1oo3/e/sPD2 Staggered	1oo2/e/PD2 Staggered	16	48	35
12	1oo2/e/sSV2 Staggered	1oo1/e/SV2 Staggered	1oo2/e/sPD2 Sequential	1oo2/e/PD2 Sequential	12	48	30

Table 11
Specification for the Pareto-front solutions.

#	PFD_{avg}	DT, h	Lifecycle cost, CU	Procurement cost, CU	Total cost of Operations, CU	Workforce-related Costs, CU	Risk costs, CU
1	$9.2181 \cdot 10^{-6}$	197	30 317 786	9 772 161	20 544 363	14 024 371	1262
2	$9.1853 \cdot 10^{-6}$	197	31 178 892	9 727 233	21 450 401	14 928 958	1258
3	$9.1488 \cdot 10^{-6}$	197	31 202 682	9 775 877	21 425 553	14 883 184	1253
4	$8.4854 \cdot 10^{-6}$	260	34 700 502	9 698 646	25 000 694	17 601 305	1162
5	$3.5302 \cdot 10^{-6}$	266	35 718 252	9 723 766	25 994 003	17 056 373	484
6	$3.5279 \cdot 10^{-6}$	266	36 819 106	9 735 046	27 083 577	18 093 924	483
7	$2.6518 \cdot 10^{-6}$	273	35 308 585	9 735 585	25 572 637	15 236 300	363
8	$2.6503 \cdot 10^{-6}$	273	38 897 801	9 797 417	29 100 021	18 549 487	363
9	$2.6503 \cdot 10^{-6}$	273	39 353 504	9 824 385	29 528 756	18 649 754	363
10	$2.6517 \cdot 10^{-6}$	273	38 428 181	9 822 473	28 605 345	18 054 689	363
11	$2.6502 \cdot 10^{-6}$	273	40 620 721	9 916 633	30 703 725	19 774 494	363
12	$2.3439 \cdot 10^{-6}$	280	38 087 311	9 767 393	28 319 597	16 759 930	321

- One may observe that the redundancy chosen for the actuator subsystems is not quite as high as that for the sensor subsystems. There are 8–10 devices in the level transmitter and fire detector subsystems, whereas there are 4–5 devices in each valve and pump drive subsystem. This result may be attributed to good reliability performance indicators of the chosen smart actuators.

Based on Table 11, several observations are made with respect to the values of the three objective functions employed for this decision-making and also, with respect to the cost structure of the produced solutions.

- The required SIL for this engineering solution is 3. It corresponds to values of the PFD_{avg} lower than 10^{-3}. All of the Pareto-front solutions satisfy this requirement. The produced results would also satisfy the requirements for SIL4.
- The lifecycle cost values range from approximately 30 to 40 mln currency units. Such a difference in costs is a matter for the stakeholders to consider carefully while the requirements to the planned solutions are formulated, and the stakeholder's viewpoints on the engineering design are considered.
- The values of the expected facility downtime range from 197 to 280 h. One may also observe that in the produced results, this objective, though being of technological or safety nature, appears consistent with the lifecycle cost criterion. It may be attributed to the considerable role of the planned periodic maintenance in the overall downtime evaluation, while the role of the safety system failures becomes less significant given the notable safety level achieved in the presented results.
- The overhaul period appears to have a considerable bearing on the facility downtime. Longer downtime corresponds to more frequent overhauls. For solution 1–3, the overhaul period is 52 weeks and the expected downtime is approximately 197 h. For the remaining solutions, the overhaul period is 48 weeks and the downtime ranges from 260 to 280 h. This variation may be attributed to the variation in TI, where shorter TI corresponds to longer downtime.
- In addition to the values of the three objective functions used in this decision-making framework, Table 11 demonstrates the cost breakdown for the Pareto-front solution. Among the presented costs, one may observe that the workforce-related costs constitute a considerable share of the lifecycle cost (at least 40%). It proves the importance of having proper workforce organization for planning maintenance in remote locations.
- Another considerable component of the operational expenditures is the production losses due to the facility downtime. This cost component accounts for 20%–30% of the cost of operations.
- Notably low risk costs may be attributed to the low PFD_{avg} values in the results, which in turn are due to the implementation of diverse redundancy in the SIS's architecture creating sufficient safety barriers and mitigating risk of the unwanted hazardous events.

The following observations are made with respect to the revealed tendencies regarding maintenance planning and workforce organization.

- Among the Pareto-front solutions, the test interval varies significantly from 12 weeks (approximately four months) to 52 weeks (one year). At the same time, the chosen overhaul period is rather large and it ranges from 48 to 52 weeks. Such a considerably long period between the overhauls is allowed due to the notably good SIS performance results in terms of reliability. The values of the PFD_{avg} are much lower than required by the regulations.
- From Table 10, sequential and staggered testing policies are chosen for periodic maintenance, while the parallel testing is never chosen. This result is attributed to the fact that sequential and staggered testing is conducted while the operations are running. Parallel testing, on the other hand, requires the process shutdown, and so, the parallel testing policy is never chosen to avoid more downtime, and by extension, larger production losses.
- For the largest overhaul period of one year (solutions 1–3), the results suggest that staggered testing is the best fit. For the shorter overhaul period (48 weeks, solutions 4–12), sequential testing is generally preferred, except for the safety valves, for which staggered policy is still chosen.
- The choices of the maintenance policies may be attributed to the optimization algorithm's attempt to organize the maintenance in such a way that during the normal course of operations there is a rather stable demand for the number of employees to be constantly present at the facility (which, in this example, is 3–4 crews), and only during the full facility overhauls, more workers are required (in this example, 10–11 crews).
- The staff size of maintenance engineers (hired and trained at the local subsidiary) required to conduct the maintenance at the remotely-located facility is provided in Table 10. A closer look at the employee scheduling results (values of $y_{l,s}^{travel}$ from the employee scheduling modeling block) shows that for the normal course of operations, 4-week trips with 8-hour daily schedule (3-worker crews) are preferred. For the weeks, when the overhauls are conducted, 1-week trips with 12-hour daily schedule (2-worker crews) are chosen to cover the surge in demand for maintenance engineers.

5. Conclusions

This research focuses on issues of safety instrumented systems design, planning their maintenance, and scheduling the workforce to conduct the necessary maintenance in remotely located O&G industrial facilities. The objective has been to plan a set of technical and organizational measures for the SISs to ensure the production processes' safety and continuity. This paper presents a multi-objective decision-making framework covering certain important aspects of the SIS solution.

This research has demonstrated the possibility of incorporating complex real-life maintenance policies (parallel, sequential, and staggered) into a Markov model of SIS functioning, which has not been explored well in literature. The use of diverse redundancy for the field instrumentation has proved beneficial in terms of the achieved safety performance. This research has also elaborated on the employee scheduling model by considering the trips and daily working schedules, as well as limiting the time the employees have to spend at the remote location during each year.

From the analysis of the obtained solutions, the *advisable instrumentation is narrowed down*; the *advisable architectures are suggested*, and also, the *maintenance strategy is selected*. The latter includes the frequency of periodic inspections and the proof testing policy suitable for the remotely-located facility. By the case example demonstrated in the paper, one may conclude that it is *possible to use the results* to facilitate formulating *comprehensive and straightforward requirements specification for the SIS*, which is designed to ensure the safety of a particular technology. The obtained recommendations may be used by both E&P operators and engineering contractors while negotiating the requirement specification for the automated process control systems. These recommendations are a good starting point for the detailed engineering design, which is the most important practical implication of this research.

The main limitation of this research is that the received results do not apply to all possible scenarios of SIS deployment due to their variety of instrumentation, designs, processes, as well as the diversity of devices and technologies used for the SIS design. In other words, the demonstrated results may not be considered generalizable for any hazardous industrial process. It may also be deduced from every particular company's organizational experience. Nevertheless, the developed decision-making framework may be used to produce at least some conclusions in each separate case it is applied to.

One of the directions for further research in this area may be to incorporate additional (more complex) maintenance policies, such as

various scenarios of partial proof-testing. Another direction to elaborate the presented decision-making framework is to study various contexts of remotely-located facilities, such as offshore installations, onshore remote facilities, the Arctic environment, and so on. The details of these problem contexts may help identify relevant issues for elaborating the workforce organization modeling block. A more comprehensive employee scheduling model may be developed, for example, by including the choice of transportation mode as a decision variable if several options are available. Further research in this area may also benefit from examining the mentioned issues through theoretical lenses of project management in the oil and gas industry. This type of research may be organized in the form of case studies.

CRediT authorship contribution statement

Yury Redutskiy: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Resources, Software, Supervision, Validation, Visualization, Writing - original draft, Review & editing. **Cecilie M. Camitz-Leidland:** Investigation, Software. **Anastasiia Vysochyna:** Investigation, Software. **Kristanna T. Anderson:** Investigation, Software. **Marina Balycheva:** Resources, Validation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Conley HA. A new security architecture for the Arctic. In: Center for strategic and international studies (CSIS). 2012.

[2] Devold H. Oil and gas production handbook: an introduction to oil and gas production. ABB; 2013.

[3] Centre for Chemical Process Safety (CCPS). Guidelines for safe process operations and maintenance. John Wiley & Sons; 2010.

[4] Gruhn P, Cheddie H. Safety shutdown systems: Design, analysis and justification. NC: The Instrumentation Systems and Automation Society; 2006.

[5] Redutskiy Y. Optimization of safety instrumented system design and maintenance frequency for oil and gas industry processes. Manage Prod Eng Rev 2017a;8(1):46–59.

[6] Redutskiy Y. Modelling and design of Safety Instrumented Systems for upstream processes of petroleum sector. Procedia Eng 2017b;182:611–8.

[7] Health and Safety Executive (HSE). Out of control. 2nd ed.. UK: HSE Books; 2003.

[8] Scientific Technical Center (STC) of Industrial Safety. Federal law on industrial safety of hazardous production facilities. Moscow, Russia.: STC Industrial safety CJSC; 2014.

[9] Norwegian Oil and Gas (NOG) Association, 2018. 070 – Application of IEC61508 and IEC61511 in the Norwegian Petroleum Industry, Norwegian Oil and Gas. Sandnes, Norway.

[10] Bourmistrov A, Mellemvik F, Bambulyak A, Gudmestad O, Overland I, Zolotukhin A, editors. International arctic petroleum cooperation: Barents sea scenarios. Routledge; 2015.

[11] Redutskiy Y. Pilot study on the application of employee scheduling for the problem of safety instrumented system design and maintenance planning for remotely located oil and gas facilities. Eng Manage Prod Serv 2018;10(4):55–64.

[12] International Electrotechnical Commission (IEC) 61508. Functional safety of electrical/electronic/programmable electronic safety related systems. Geneva, Switzerland: IEC; 1998/2010.

[13] International Electrotechnical Commission (IEC) 61511. Functional safety - safety instrumented systems for the process industry. Geneva, Switzerland: IEC; 2003/2016.

[14] Bukowski JV. Using Markov models to compute probability of failed dangerous when repair times are not exponentially distributed. In: RAMS'06. Annual reliability and maintainability symposium. IEEE; 2006, p. 273–7.

[15] Jin H, Lundteigen MA, Rausand M. Reliability performance of safety instrumented systems: A common approach for both low-and high-demand mode of operation. Reliab Eng Syst Saf 2011;96(3):365–73.

[16] Mechri W, Simon C, BenOthman K. Switching Markov chains for a holistic modeling of SIS unavailability. Reliab Eng Syst Saf 2015;133:212–22.

[17] Srivastav H, Barros A, Lundteigen MA. Modelling framework for performance analysis of SIS subject to degradation due to proof tests. Reliab Eng Syst Saf 2020;195:106702.

[18] Kuo Way, Zuo Ming J. Optimal reliability modeling. In: Principles and applications. 2003.

[19] Gabriel A, Ozansoy C, Shi J. Developments in SIL determination and calculation. Reliab Eng Syst Saf 2018;177:148–61.

[20] Torres-Echeverria AC, Martorell S, Thompson HA. Design optimization of a safety-instrumented system based on RAMS+C addressing IEC 61508 requirements and diverse redundancy. Reliab Eng Syst Saf 2009;94(2):162–79.

[21] Ouyang Z, Liu Y, Ruan SJ, Jiang T. An improved particle swarm optimization algorithm for reliability-redundancy allocation problem with mixed redundancy strategy and heterogeneous components. Reliab Eng Syst Saf 2019;181:62–74.

[22] Dobani ER, Ardakan MA, Davari-Ardakani H, Juybari MN. RRAP-CM: A new reliability-redundancy allocation problem with heterogeneous components. Reliab Eng Syst Saf 2019;191:106563.

[23] Littlewood B. The impact of diversity upon common mode failures. Reliab Eng Syst Saf 1996;51(1):101–13.

[24] Van der Meulen M. On the use of smart sensors, common cause failure and the need for diversity. In: 6th international symposium programmable electronic systems in safety related applications. TUV.; 2004.

[25] Khatab A, Nahas N, Nourelfath M. Availability of K-out-of-N: G systems with non-identical components subject to repair priorities. Reliab Eng Syst Saf 2009;94(2):142–51.

[26] Ding L, Wang H, Jiang J, Xu A. SIL verification for SRS with diverse redundancy based on system degradation using reliability block diagram. Reliab Eng Syst Saf 2017;165:170–87.

[27] Hadipour H, Amiri M, Sharifi M. Redundancy allocation in series-parallel systems under warm standby and active components in repairable subsystems. Reliab Eng Syst Saf 2019;192:106048.

[28] Dantzig GB. Letter to the editor – A comment on Edie's 'Traffic delays at toll booths'. J Oper Res Soc Amer 1954;2(3):339–41.

[29] Van den Bergh J, Beliën J, De Bruecker P, Demeulemeester E, De Boeck L. Personnel scheduling: A literature review. European J Oper Res 2013;226(3):367–85.

[30] Castillo-Salazar JA, Landa-Silva D, Qu R. Workforce scheduling and routing problems: literature survey and computational study. Ann Oper Res 2016;239(1):39–67.

[31] Soriano J, Jalao ER, Martinez IA. Integrated employee scheduling with known employee demand, including breaks, overtime, and employee preferences. J Ind Eng Manage 2020;13(3):451–63.

[32] Helber S, Henken K. Profit-oriented shift scheduling of inbound contact centers with skills-based routing, impatient customers, and retrials. OR Spectrum 2010;32(1):109–34.

[33] Goble WM. Control systems safety evaluation and reliability. 3rd ed.. Research Triangle Park: ISA; 2010.

[34] Deb K. Multi-objective optimization using evolutionary algorithms. John Wiley & Sons; 2001.